

Docket No. AUS920010388US1

CLAIMS:

What is claimed is:

5

1. A method of encrypting data, the data being comprised of a plurality of data chunks, comprising:
 encrypting each of the plurality of data chunks;
 calculating a plurality of intermediate digital digests
 10 based on the encrypted data chunks, each intermediate digital digest being associated with one or more of the data chunks; and

 formulating a data package comprising the encrypted data chunks and the plurality of intermediate digital
 15 digests.

2. The method of claim 1, wherein each of the intermediate digital digests corresponds to a more than one data chunk.

20 3. The method of claim 1, wherein each intermediate digital digest builds from a previously calculated intermediate digital digest.

4. A method of decrypting an encrypted data package, the
 25 encrypted data package being comprised of a plurality of encrypted data portions, comprising:

 reading an encrypted data portion from the plurality of encrypted data portions;

 calculating a calculated digital digest for the
 30 encrypted data portion;

 decrypting an intermediate digital digest from the encrypted data package; and

09881921-061401
 T-03-01-01

Docket No. AUS920010388US1

authenticating the encrypted data portion based on a comparison of the intermediate digital digest to the calculated digital digest.

5 5. The method of claim 4, wherein if the intermediate digital digest matches the calculated digital digest, the encrypted data portion is authentic.

6. The method of claim 5, wherein if the encrypted data
10 portion is authentic, the method further comprises:
decrypting the encrypted data portion; and
repeating the steps of reading, decrypting and
authenticating for a next encrypted data portion of the data
package.

15 7. The method of claim 4, wherein the intermediate digital digest corresponds to an amount of data different from an amount of data in the encrypted data portion.

20 8. The method of claim 4, wherein decrypting an intermediate digital digest from the encrypted data package includes reading an intermediate digital digest from a digital digest portion of the encrypted data package, the digital digest portion having a plurality of intermediate
25 digital digests arranged in an order.

9. The method of claim 8, wherein the intermediate digital digest is built up from a previous intermediate digital digest in the order.

Docket No. AUS920010388US1

10. The method of claim 8, wherein the intermediate digital
digest corresponds to a different amount of encrypted data
than other intermediate digital digests in the digital
5 digest portion.

11. An apparatus for encrypting data, the data being
comprised of a plurality of data chunks, comprising:
means for encrypting each of the plurality of data
10 chunks;

means for calculating a plurality of intermediate
digital digests based on the encrypted data chunks, each
intermediate digital digest being associated with one or
more of the data chunks; and

15 means for formulating a data package comprising the
encrypted data chunks and the plurality of intermediate
digital digests.

12. The apparatus of claim 11, wherein each of the
20 intermediate digital digests corresponds to a more than one
data chunk.

13. The apparatus of claim 11, wherein each intermediate
digital digest builds from a previously calculated
25 intermediate digital digest.

14. An apparatus of decrypting an encrypted data package,
the encrypted data package being comprised of a plurality of
encrypted data portions, comprising:
30 means for reading an encrypted data portion from the
plurality of encrypted data portions;

Docket No. AUS920010388US1

means for calculating a calculated digital digest for the encrypted data portion;

means for decrypting an intermediate digital digest from the encrypted data package; and

- 5 means for authenticating the encrypted data portion based on a comparison of the intermediate digital digest to the calculated digital digest.

15. The apparatus of claim 14, wherein if the intermediate
10 digital digest matches the calculated digital digest, the encrypted data portion is authentic.

16. The apparatus of claim 15, further comprising:

means for decrypting the encrypted data portion; and

- 15 means for invoking the means for reading, means for decrypting and means for authenticating for a next encrypted data portion of the data package, wherein the means for decrypting the encrypted data portion and the means for invoking operate if the encrypted data portion is authentic.

20

17. The apparatus of claim 14, wherein the intermediate digital digest corresponds to an amount of data different from an amount of data in the encrypted data portion.

- 25 18. The apparatus of claim 14, wherein the means for decrypting an intermediate digital digest from the encrypted data package includes means for reading an intermediate digital digest from a digital digest portion of the encrypted data package, the digital digest portion having a
30 plurality of intermediate digital digests arranged in an order.

Docket No. AUS920010388US1

19. The apparatus of claim 18, wherein the intermediate digital digest is built up from a previous intermediate digital digest in the order.

5 20. The apparatus of claim 18, wherein the intermediate digital digest corresponds to a different amount of encrypted data than other intermediate digital digests in the digital digest portion.

10 21. A computer program product of encrypting data, the data being comprised of a plurality of data chunks, comprising:

first instructions for encrypting each of the plurality of data chunks;

15 second instructions for calculating a plurality of intermediate digital digests based on the encrypted data chunks, each intermediate digital digest being associated with one or more of the data chunks; and

third instructions for formulating a data package comprising the encrypted data chunks and the plurality of
20 intermediate digital digests.

22. The computer program product of claim 21, wherein each of the intermediate digital digests corresponds to a more than one data chunk.

25

23. The computer program product of claim 21, wherein each intermediate digital digest builds from a previously calculated intermediate digital digest.

30 24. A computer program product of decrypting an encrypted data package, the encrypted data package being comprised of a plurality of encrypted data portions, comprising:

0983491-061401
T04790-T26860

Docket No. AUS920010388US1

first instructions for reading an encrypted data portion from the plurality of encrypted data portions;

second instructions for calculating a calculated digital digest for the encrypted data portion;

5 third instructions for decrypting an intermediate digital digest from the encrypted data package; and

fourth instructions for authenticating the encrypted data portion based on a comparison of the intermediate digital digest to the calculated digital digest.

10

25. The computer program product of claim 24, wherein if the intermediate digital digest matches the calculated digital digest, the encrypted data portion is authentic.

15 26. The computer program product of claim 25, further comprising:

fifth instructions for decrypting the encrypted data portion; and

20 Sixth instructions for repeating execution of the first, second, third and fourth instructions for a next encrypted data portion of the data package, if the encrypted data portion is authentic.

27. The computer program product of claim 24, wherein the 25 intermediate digital digest corresponds to an amount of data different from an amount of data in the encrypted data portion.

28. The computer program product of claim 24, wherein the 30 third instructions for decrypting an intermediate digital digest from the encrypted data package include instructions for reading an intermediate digital digest from a digital

0988191-051401

Docket No. AUS920010388US1

digest portion of the encrypted data package, the digital digest portion having a plurality of intermediate digital digests arranged in an order.

5 29. The computer program product of claim 28, wherein the intermediate digital digest is built up from a previous intermediate digital digest in the order.

30. The computer program product of claim 28, wherein the
10 intermediate digital digest corresponds to a different amount of encrypted data than other intermediate digital digests in the digital digest portion.

TELETYPE UNIT